INFORMATION ABOUT SECURITY OF

PROFESSIONAL OLYMPUS DICTATION SOLUTIONS

General

Olympus offers - as the global market leader of dictation - to encrypt the whole workflow of a dictation from creation to transcription and thereby prevent unauthorised access.

The backup includes the dictation device (the hardware) as well as the Olympus dictation management software. The backup can cover up to five areas:

1. access to the dictation device
2. access control of files on the memory
3. dictation encryption of dictations when transferring
4. prevent files against accidental deletion: dictation device
5. prevent files against accidental deletion: dictation software
6. backup of dictations via dictation management software
7. security through ease of use
8. security by IT environment: Thin-Clients

1. Access to Dictation Device

The Olympus dictation devices **DS-5000** and **DS-3400** offers the possibility to access using optionally a 4-digit PIN code to encrypt.

Thus, there is no opportunity for unauthorised persons, with the dictation device to record dictations, play or edit.

The activation of this function is recommended if the risk exists that unauthorised access to the dictation of the relevant dictators could happen (for example, if it could happen that people leave their dictation devices on desk at offices).

The Olympus dictation device **DS-5000iD** also offers the possibility to control the access to the dictation device via biometric information (fingerprint recognition). On the one hand the use for the authorised user is even easier. On the other hand, this solution has the advantage that the authorised user does not have to remember the PIN code and an unauthorised user has no access to the device even he knows the PIN code.

Up to 10 different authors for each device can be managed.

2. Access to files on the memory

Olympus uses in his professional dictation devices DS-5000iD, DS-5000 and DS-3400 the international dictation standard “**DSS Pro**” with all functionalities. One of the advantages includes strong compression, editing and dictation categorisation using various attributes.

By DSSPro format, the already high-quality audio with a 16kHz sampling rate further improved (enables optimised use of speech recognition systems), and it is the first time an encryption algorithm is supported.

This optional **encryption** is possible for one or all **folders** of the dictation device[1].

If an unauthorised removes one or both[2] memory cards of Olympus dictation devices 5000iD, DS-5000 or DS-3400, no access, play or editing of stored data stored on the dictation devices are possible.

This encryption is done in real time on the dictation device. Using the Dictation Management Software “DSS Player Pro” for each folder of the dictation devices an individually password can be stored. All recordings in this folder will be then encrypted. To play back these recordings it is necessary to enter the decryption password or to deposit this password in the inbox of the responsible typist.

3. Dictation encryption of dictations when transferring

When dictations are downloaded (manually or automatically) from the dictation devices and sent to an authorised person (internal or external transcriptionists), there is a third security level when using the Olympus Dictation Management Software “**DSS Player Pro R5**".

Every dictator can individually encrypt in the “**DSS Player Pro Dictation Module**” a single dictation manually or all dictations automatically with workflow rules via password on the way to other parties.

The decryption is done on the typist side in "**DSS Player Pro R5 Transcription Module**”, either manually or automatically by setting any number of author profiles. This

[1] The number of folders can be individually selected (1-7 folders).
[2] DS-5000iD and DS-5000 support 2 memory cards, DS-3400 one.

is particularly advantageous when - as often in practice - a typist is active for several dictators.

Olympus is using for this encryption / decryption the 128-bit Advanced Encryption Standard (AES) - Technology.

The **Advanced Encryption Standard (AES)** is a symmetric crypto system, as the successor for DES and 3DES in October 2000 by the National Institute of Standards and Technology (NIST) as standard was announced, worldwide in use.

The standard provides a very high degree of safety. The procedure was taken under detailed cryptanalytic tests.

AES is approved in the USA for governmental documents with the highest level of secrecy!

The official specification of the AES by NIST can be found in the Appendix.

In addition, various automatic download options can be setup. Among other things e.g. a dictation can be automatically erased on the dictation device by the Olympus dictation management software, if the complete download to the PC was successful. This ensures that dictations are no longer located on the dictation devices, which already have been completed and are already in the transcription status.

When using a device by several authors is thus automatically ensured that no foreign dictations are left on the device, when the next author starts to work.

4. Prevent files against accidental deletion: dictation device

If necessary, a single file on the device can be protected with an **erase lock** against accidental deletion.

5. Prevent files against accidental deletion: dictation software

In the Olympus dictation management software an option can be activated, that dictations are not fully erased immediately but will be transferred first to the Windows Recycle Bin.

A final erase of the dictations is then done only when the Windows function “Empty Recycle Bin” will be used.

6. Backup of dictations via dictation management software

There is a backup function which can be activated in the Olympus dictation management software, which is doing a **security backup** of each dictation. To limit the memory requirement, an optional **automatic erase logic** can be activated (e.g. erase dictations automatically after 7 days).

7. Security through ease of use

Olympus dictation devices and software have very good ergonomics. By **individually definable menus** (central administration) operating errors are eliminated as far as possible. The dictator can only see and adjust what he is also allowed to see and adjust.

8. Security by IT environment: Thin-Clients

Olympus supports via specially developed drivers, integrations and cooperations with Thin-Client manufacturers the ability of run of professional Olympus dictation devices in Thin Client environments.

Thin Clients offer several advantages: Beside low **acquisition**- and maintenance costs vs. Fat Clients a high **data security and data integrity** is ensured because the dictations are not saved locally anymore.

Note: PC access is controlled by the user (hard disk - operating system-access, other passwords).